Chapitre 20. Arithmétique

I. Divisibilité dans $\mathbb{Z}$

1) Définition de la divisibilité dans $\mathbb{Z}$

Définition 1. Soient a et b deux entiers relatifs tels que $a \neq 0$.
On dit que a **divise** b si et seulement si il existe un entier relatif q tel que $b = qa$.
Il revient au même de dire a divise b ou b est **divisible par** a ou b est **multiple** de a.
Quand a divise b, on écrit $a \mid b$ et quand a ne divise pas b, on écrit $a \nmid b$

Exemples. 2 divise 6 car $6 = 3 \times 2$ avec 3 entier relatif. 4 divise -4 car $4 = (-1) \times (-4)$ avec -1 entier relatif. 1 divise 5 car $5 = 5 \times 1$ avec 5 entier relatif. 1 divise 0 car $0 = 0 \times 1$ avec 0 entier relatif.

Remarque 1. Dans la définition 1, on a imposé à a d'être non nul ou encore on n'écrira jamais une phrase du genre « 0 divise ... ». Néanmoins, puisque $0 = 0 \times 0$, on peut se permettre de dire que 0 est un multiple de 0 (mais pas que 0 est un diviseur de 0).

Remarque 2. Si a est un entier relatif, les multiples de l'entier a sont les entiers relatifs de la forme $q \times a$ où q est un entier relatif. Ce sont donc les nombres

$$\ldots \quad -3a \quad -2a \quad -a \quad 0 \quad a \quad 2a \quad 3a \quad \ldots$$

Par exemple, les multiples de 3 sont les entiers relatifs

$$\ldots \quad -9 \quad -6 \quad -3 \quad 0 \quad 3 \quad 6 \quad 9 \quad \ldots$$

Exercice 1. Montrer par récurrence que pour tout entier naturel non nul n, $3^{4n-1} + 3$ est divisible par 5.

Solution. Montrons par récurrence que pour tout entier naturel non nul n, $3^{4n-1} + 3$ est divisible par 5.

- $3^{4\times1-1} + 3 = 3^3 + 3 = 30 = 6 \times 5$ et donc la propriété est vraie quand $n = 1$.
- Soit $n \geqslant 1$. Supposons que $3^{4n-1} + 3$ soit divisible par 5 et montrons que $3^{4(n+1)-1} + 3$ est divisible par 5.

$$3^{4(n+1)-1} + 3 = 3^{4n-1} \times 3^4 + 3 = (3^{4n-1} + 3) \times 3^4 - 3 \times 3^4 + 3 = (3^{4n-1} + 3) \times 3^4 - 240.$$

Par hypothèse de récurrence, il existe un entier relatif k tel que $3^{4n-1} + 3 = 5k$. On en déduit que

$$3^{4(n+1)-1} + 3 = 5k \times 3^4 - 240 = 5k \times 81 - 5 \times 48 = 5(81k - 48).$$

Puisque $81k - 48$ est un entier relatif, on a montré que $3^{4(n+1)-1} + 3$ est divisible par 5.

Le résultat est démontré par récurrence.

Commentaire. Un moment important de la solution ci-dessus est le moment où on dit que « $81k - 48$ est un entier relatif ». On ne peut pas se contenter d'écrire $3^{4(n+1)-1} + 3 = 5(81k - 48)$ sans préciser que $81k - 48$ est un entier relatif. Si cette phrase n'est pas écrite, la solution ne vaut rien.
Par exemple, il existe q tel que $3 = 2q$ à savoir $q = \dfrac{3}{2}$ mais en aucune façon l'entier 2 ne divise l'entier 3. Le problème est que $q = \dfrac{3}{2}$ n'est pas un entier. ❑

Théorème 1. Soit a un entier naturel non nul. Tout diviseur de a est inférieur ou égal à a.

Démonstration. Soient a un entier naturel non nul puis d un entier relatif non nul qui est un diviseur de a.

Si $d < 0$, alors $d \leqslant a$ car $a > 0$.

Supposons maintenant $d > 0$. Il existe un entier relatif q tel que $a = q \times d$. Puisque $q = \dfrac{a}{d}$, q est strictement positif et donc q est un entier naturel non nul. En particulier, $q \geqslant 1$. On en déduit que

$$a = q \times d \geqslant 1 \times d = d.$$

On a montré que tout diviseur de a est inférieur ou égal à a.

Remarque. Le résultat est faux si $a = 0$ car par exemple 1 divise 0, puisque $0 = 0 \times 1$, mais $1 > 0$. ❏

Théorème 2. Soit a un entier relatif.
Les diviseurs de a sont les diviseurs de $|a|$.

Démonstration. Soit a un entier relatif.

Si $a \geqslant 0$, alors $|a| = a$ et il n'y a rien à démontrer.

Supposons maintenant $a < 0$. Alors, $|a| = -a$. Soit d un entier relatif non nul.
Si d divise a, il existe un entier relatif q tel que $a = q \times d$. Mais alors, $-a = (-q) \times d$ avec $-q$ entier relatif. On en déduit que d divise $-a$.
Si d divise $-a$, il existe un entier relatif q tel que $-a = q \times d$. Mais alors, $a = (-q) \times d$ avec $-q$ entier relatif. On en déduit que d divise a.

Finalement, les diviseurs de a sont les diviseurs de $|a|$.

Commentaire. Ce résultat ramène les problèmes de divisibilité entre entiers relatifs à des problèmes de divisibilité entre entiers naturels. ❏

2) Propriétés de la divisibilité

Théorème 3. **1)** Pour tout entier relatif non nul a, a divise 0 ou aussi 0 est un multiple de a.

2) Pour tout entier relatif a, 1 divise a ou aussi a est un multiple de 1.

Démonstration. 1) Soit a un entier relatif non nul. On a $0 = 0 \times a$ et puisque 0 est un entier relatif, on a montré que a divise 0.

2) Soit a un entier relatif. On a $a = a \times 1$ et puisque a est un entier relatif, on a montré que 1 divise a.

Théorème 4. **1) a)** Pour tout entier naturel non nul a, a divise a ou aussi a est un multiple de a.
b) Pour tout entier relatif non nul a, a divise a, a divise $-a$, $-a$ divise a et $-a$ divise $-a$.

2) a) Soient a et b deux entiers naturels non nuls. a divise b et b divise a si et seulement si $b = a$.
b) Soient a et b deux entiers relatifs non nuls. a divise b et b divise a si et seulement si $b = a$ ou $b = -a$.

3) Soient a, b et c trois entiers relatifs tels que $a \neq 0$ et $b \neq 0$. Si a divise b et b divise c alors a divise c.

Démonstration. 1) a) et b) Soit a un entier relatif non nul. On a $a = 1 \times a$ et puisque 1 est un entier relatif, on a montré que a divise a. En appliquant ce résultat à l'entier relatif $-a$ qui n'est pas nul, on a aussi montré que $-a$ divise $-a$.
De même, les égalités, $-a = (-1) \times a$ et $a = (-1) \times (-a)$ montrent respectivement que a divise $-a$ et $-a$ divise a.

2) a) Soient a et b deux entiers naturels non nuls tels que a divise b et b divise a.

Alors, il existe un entier relatif q_1 tel que $b = q_1 a$ et un entier relatif q_2 tel que $a = q_2 b$.
Puisque $q_1 = \dfrac{b}{a}$, q_1 est strictement positif et donc q_1 est un entier naturel non nul. De même, q_2 est un entier naturel non nul. On en déduit que $q_1 \geqslant 1$ et $q_2 \geqslant 1$.
Puisque $b = q_1 a$ et $a = q_2 b$, on a $a = q_2(q_1 a) = (q_1 q_2)a$ et puisque a n'est pas nul, on en déduit que $q_1 q_2 = 1$.

En résumé, q_1 et q_2 sont deux entiers supérieurs ou égaux à 1 dont le produit $q_1 q_2$ est égal à 1. Si l'un de ces deux entiers n'est pas égal à 1, alors l'un de ces deux entiers est au moins égal à 2 puis le produit $q_1 q_2$ est au moins égal à $2 \times 1 = 2$. Ceci est faux et donc les deux entiers q_1 et q_2 sont égaux à 1. Mais alors $b = a$.

Réciproquement, si $b = a$, alors a divise b et b divise a d'après 1).

On a montré que pour tous entiers naturels non nuls a et b, a divise b et b divise a si et seulement si $b = a$.

b) Soient a et b deux entiers relatifs non nuls tels que a divise b et b divise a.

Il existe donc un entier relatif q_1 tel que $b = q_1 a$ et un entier relatif q_2 tel que $a = q_2 b$. Mais alors $|b| = |q_1| \times |a|$ et $|a| = |q_2| \times |b|$. Ainsi, $|a|$ et $|b|$ sont deux entiers naturels non nuls tels que $|a|$ divise $|b|$ et $|b|$ divise $|a|$. D'après 2)a), on a nécessairement $|b| = |a|$ puis $b = a$ ou $b = -a$.

Réciproquement, si $b = a$ ou $b = -a$, alors a divise b et b divise a d'après 1).

On a montré que pour tous entiers relatifs non nuls a et b, a divise b et b divise a si et seulement si $b = a$ ou $b = -a$.

3) Soient a, b et c trois entiers relatifs tels que $a \neq 0$, $b \neq 0$, a divise b et b divise c.
Il existe un entier relatif q_1 et un entier relatif q_2 tels que $b = q_1 a$ et $c = q_2 b$. Mais alors $c = q_2(q_1 a) = (q_1 q_2)a$.

Puisque q_1q_2 est un entier relatif, on en déduit que a divise c.

Théorème 5. Soient a et b deux entiers relatifs et d un entier relatif non nul.
1) Si d divise a et b, d divise $a+b$ et $a-b$.
2) Si d divise a et d divise b, alors pour tous entiers relatifs u et v, d divise $u\times a+v\times b$.

Démonstration. Le 1) est un cas particulier du 2), énoncé explicitement (ce sont les cas $u=v=1$ et $u=-v=1$). Montrons donc 2).

Soient a et b deux entiers relatifs et d un entier relatif non nul tels que d divise a et d divise b.
Il existe un entier relatif q_1 tel que $a=q_1\times d$ et il existe un entier relatif q_2 tel que $b=q_2\times d$.

Soient u et v deux entiers relatifs. Alors,

$$u\times a+v\times b=u\times q_1\times d+v\times q_2\times d=(u\times q_1+v\times q_2)d.$$

Puisque $u\times q_1+v\times q_2$ est un entier relatif, on a montré que d divise $u\times a+v\times b$.

Exercice 2. Trouver tous les entiers relatifs n tels que $n+2$ divise $2n+7$.

Solution. Soit n un entier naturel tel que $n+2$ divise $2n+7$.

Alors, comme $n+2$ divise $n+2$, $n+2$ divise aussi $(2n+7)-2(n+2)=3$ et donc $n+2\in\{-3;-1;1;3\}$ puis $n\in\{-5;-3;-1,1\}$.

Réciproquement,

- si $n=-5$, $n+2=-3$ et $2n+7=-3$. Dans ce cas, $n+3$ divise $2n+7$.
- si $n=-3$, $n+2=-1$ et $2n+7=1$. Dans ce cas, $n+3$ divise $2n+7$.
- si $n=-1$, $n+2=1$ et $2n+7=5$. Dans ce cas, $n+3$ divise $2n+7$.
- si $n=1$, $n+2=3$ et $2n+7=9$. Dans ce cas, $n+3$ divise $2n+7$.

Les entiers relatifs n tels que $n+2$ divise $2n+7$ sont -5, -3, -1 et 1.

Théorème 6. Soient a un entier relatif et d un entier relatif non nul.
Si d divise a, alors pour tout entier relatif b, d divise $a\times b$ ou encore si d divise a, alors d divise tout multiple de a.

Démonstration. Soient a un entier relatif et d un entier relatif non nul tels que d divise a.
Il existe un entier relatif q tel que $a=q\times d$. Soit alors b un entier relatif. On a $ab=(qd)b=(qb)d$. Puisque qb est un entier relatif, ceci montre que d divise ab.

II. Division euclidienne

Théorème 7 (division euclidienne d'un entier naturel par un entier naturel non nul).
Soient a un entier naturel et b un entier naturel non nul.
Il existe un couple d'entiers naturels (q,r) et un seul tel que

$$a=bq+r \text{ et } 0\leqslant r<b.$$

Démonstration. Soient a un entier naturel et b un entier naturel non nul.

Existence. Soit q la partie entière de $\dfrac{a}{b}$ puis $r=a-bq$. q est un entier naturel et r est un entier relatif.

q est le plus grand entier naturel inférieur ou égal à $\dfrac{a}{b}$ et donc $q\leqslant\dfrac{a}{b}<q+1$. En multipliant les trois membres de cet encadrement par l'entier strictement positif b, on obtient $qb\leqslant a<qb+b$ puis en retranchant le nombre bq aux trois membres de l'encadrement, on obtient $0\leqslant a-bq<b$ ou encore $0\leqslant r<b$.

Ainsi, q et r sont deux entiers naturels tels que $a=bq+r$ et $0\leqslant r<b$. Ceci montre l'existence de q et r.

Unicité. Soient q_1, q_2, r_1 et r_2 quatre entiers naturels tels que $a=bq_1+r_1=bq_2+r_2$ et $0\leqslant r_1<b$ et $0\leqslant r_2<b$.
On a en particulier $bq_1+r_1=bq_2+r_2$ puis $b(q_1-q_2)=r_2-r_1$.

Puisque $0\leqslant r_1<b$ et $0\leqslant r_2<b$, on a encore $-b\leqslant -r_1<0$ et $0\leqslant r_2<b$ puis en additionnant membre à membre, on obtient $-b<r_2-r_1<b$ ou encore $|r_2-r_1|<b$.

Supposons par l'absurde que $q_1 - q_2$ ne soit pas nul, alors $|q_1 - q_2| \geqslant 1$ puisque $q_1 - q_2$ est un entier relatif. Puisque $|r_2 - r_1| = |q_1 - q_2| \times |b| = |q_1 - q_2| \times b$, on en déduit que $|r_2 - r_1| \geqslant 1 \times b = b$ ce qui est faux.

Par suite, $q_1 - q_2 = 0$ ou encore $q_1 = q_2$ puis $r_2 - r_1 = 0$ ou encore $r_1 = r_2$. Ceci montre l'unicité de q et r.

Par exemple, la division euclidienne de 47 par 4 s'écrit

$$47 = 11 \times 4 + 3.$$

Le quotient de la division euclidienne de 47 par 4 est $q = 11$ et le reste est $r = 3$. Cette division euclidienne fournit la partie entière et la partie décimale de $\frac{47}{4}$. En effet, en divisant par 4 les deux membres de l'égalité $47 = 11 \times 4 + 3$, on obtient

$$\frac{47}{4} = 11 + \frac{3}{4},$$

où 11 est un entier et $\frac{3}{4}$ est un réel de $[0, 1[$. La division euclidienne est la division d'un entier par un autre où « on ne poursuit pas après la virgule ». Ceci est une division euclidienne

47	4
3	11

alors que ceci est une division tout court

47	4
0	11,75

Théorème 8 (division euclidienne d'un entier relatif par un entier naturel non nul).
Soient a un entier relatif et b un entier naturel non nul.
Il existe un couple d'entiers relatifs (q, r) et un seul tel que

$$a = bq + r \text{ et } 0 \leqslant r < b.$$

Démonstration. Soient a un entier relatif et b un entier naturel non nul.

Existence. Le résultat est déjà établi quand $a \geqslant 0$. Supposons $a < 0$ et posons $a' = -a$. a' est un entier naturel et on peut appliquer le théorème 5 aux entiers a et b.

Il existe deux entiers naturels q' et r' tel que $a' = bq' + r'$ et $0 \leqslant r' < b$. On a encore $a = -a' = b(-q') - r'$.
- Si $r' = 0$, on pose $q = -q'$ et $r = 0$. q et r sont des entiers relatifs tels que $a = bq + r$ et $0 \leqslant r < b$.
- Sinon, $0 < r' < b$. On écrit alors

$$a = b(-q') - r' = b(-q' - 1) + b - r'.$$

On pose $q = -q' - 1$ et $r = b - r'$. q et r sont des entiers relatifs tels que $a = bq + r$. De plus,

$$0 < r' < b \Rightarrow -b < -r' < 0 \Rightarrow b - b < b - r' < b + 0 \Rightarrow 0 < r < b \Rightarrow 0 \leqslant r < b.$$

Unicité. Elle se démontre exactement de la même façon que dans le théorème 5.

Par exemple, la division euclidienne de -47 par 4 s'écrit

$$-47 = (-12) \times 4 + 1.$$

Le quotient de cette division est $q = -12$ et le reste est $r = 1$. Cette égalité fournit de nouveau, si besoin est, la partie

entière et la partie décimale de $-\frac{47}{4}$:

$$-\frac{47}{4} = -12 + \frac{1}{4}.$$

Exercice 3. Déterminer le nombre de semaines dans une année non bissextile.

Solution. Il y a 365 jours dans une année non bissextile et 7 jours dans une semaine. La division euclidienne de 365 par 7 s'écrit

$$365 = 52 \times 7 + 1,$$

car $0 \leqslant 1 < 7$. Une année non bissextile est donc constituée de 52 semaines plus 1 jour.

On a immédiatement le résultat suivant concernant la divisibilité d'un entier par un autre :

Théorème 9. Soient a et b deux entiers relatifs tels que $b \neq 0$.
b divise a si et seulement si le reste de la division euclidienne de a par b est nul.

III. PGCD.

1) Définition du PGCD

Théorème 10. Soient a et b deux entiers relatifs tels que $a \neq 0$ ou $b \neq 0$.
L'ensemble des diviseurs communs à a et b admet un plus grand élément qui est un entier naturel.

Démonstration. Soient a et b deux entiers relatifs tels que $a \neq 0$ ou $b \neq 0$. Supposons par exemple que $a \neq 0$.

Soit D l'ensemble des diviseurs communs à a et b qui sont des entiers naturels non nuls.
D n'est pas vide car 1 est un diviseur commun à a et b qui est de plus un entier naturel non nul.

D'après les théorèmes 1 et 2, pour tout élément d de D, on a $1 \leqslant d \leqslant |a|$.

Ainsi, D est un ensemble d'entiers naturels non nuls qui contient un nombre fini d'éléments (au plus $|a|$) et donc D admet un plus grand élément ce qu'il fallait démontrer.

Remarque. Si $a = b = 0$, la notion de PGCD de a et b n'a pas de sens car tout entier relatif non nul est un diviseur commun à a et b.

Définition 2. Soient a et b deux entiers relatifs tels que $a \neq 0$ ou $b \neq 0$.
Le plus grand des divisieurs communs à a et b s'appelle le PGCD de a et b (« plus grand commun diviseur ») et se note $\mathrm{PGCD}(a, b)$.

Exemple. Le PGCD de -12 et 18 est 6. En effet, les diviseurs de -12 qui sont des entiers naturels non nuls sont

$$1,\ 2,\ 3,\ 4,\ 6 \text{ et } 12.$$

Parmi ces diviseurs, seuls 1, 2, 3 et 6 divisent aussi 18. Les diviseurs communs à -12 et 18 qui sont des entiers naturels non nuls sont donc 1, 2, 3 et 6. Le plus grand de ces diviseurs communs est 6.

2) Propriétés du PGCD

Théorème 11.
1) Soient a et b deux entiers relatifs tels que $a \neq 0$ ou $b \neq 0$.

$$\mathrm{PGCD}(a, b) = \mathrm{PGCD}(|a|, |b|).$$

Démonstration. D'après le théorème 2, les diviseurs communs à a et b sont aussi les diviseurs communs à $|a|$ et $|b|$.
En particulier, le plus grand des diviseurs communs à a et b est aussi le plus grand des diviseurs communs à $|a|$ et $|b|$ ce qui démontre le résultat.

Commentaire. Ce résultat ramène la recherche du PGCD de deux entiers relatifs à la recherche du PGCD de deux entiers naturels. ❑

Théorème 12.
1) Soit a un entier naturel non nul.

a) $\text{PGCD}(a,a) = a$.
b) $\text{PGCD}(a,1) = 1$.
c) $\text{PGCD}(a,0) = a$.

2) Soit a un entier relatif non nul.

a) $\text{PGCD}(a,a) = |a|$.
b) $\text{PGCD}(a,1) = 1$.
c) $\text{PGCD}(a,0) = |a|$.

Démonstration. D'après le théortème 10, il suffit d'étudier le cas où a est un entier naturel non nul. Soit donc a un entier naturel non nul.

D'après le théorème 1, tout diviseur commun à a et a c'est-à-dire tout diviseur de a est inférieur ou égal à a. Comme a est un diviseur de a d'après le théorème 4, a est le plus grand des diviseurs communs à a et a ou encore $a = \text{PGCD}(a,a)$.

Tout diviseur commun à a et 1 est inférieur ou égal à 1. Comme 1 est un diviseur commun à a et 1 d'après le théorème 3, 1 est le plus grand des diviseurs communs à a et 1 ou encore $1 = \text{PGCD}(a,1)$.

Tout diviseur commun à a et 0 est inférieur ou égal à a. Comme a est un diviseur commun à a et 0 d'après le théorème 3, a est le plus grand des diviseurs communs à a et 0 ou encore $a = \text{PGCD}(a,0)$.

Théorème 13.
1) Soient a et b deux entiers naturels tels que $b \neq 0$. Si b divise a, $\text{PGCD}(a,b) = b$.
2) Soient a et b deux entiers relatifs tels que $b \neq 0$. Si b divise a, $\text{PGCD}(a,b) = |b|$.

Démonstration. Encore une fois, il suffit de démontrer le théorème dans le cas où a et b sont des entiers naturels.

Soient a et b deux entiers naturels tels que $b \neq 0$ et b divise a.
Tout diviseur commun à a et b est un diviseur de b et est donc inférieur ou égal à b.
D'autre part, puisque b divise a et b divise b, b est un diviseur commun à a et b.

b est donc le plus grand des diviseurs communs à a et b ou encore $b = \text{PGCD}(a,b)$.

Théorème 14. Soient a et b deux entiers relatifs non nuls.
1) Il existe deux entiers relatifs u et v tels que $\text{PGCD}(a,b) = a \times u + b \times v$.
2) Les diviseurs communs à a et à b sont les diviseurs de leur PGCD.

Démonstration. Soient a et b deux entiers relatifs non nuls. Supposons par exemple que $|b| \leqslant |a|$.

1) Notons E l'ensemble des entiers naturels non nuls de la forme $a \times u + b \times v$ où u et v sont des entiers relatifs et qui sont inférieurs ou égaux à $|b|$ (et donc à $|a|$). E n'est pas vide car si $b > 0$, pour $u = 0$ et $v = 1$, on obtient $a \times u + b \times v = b = |b|$ qui est un entier naturel non nul inférieur ou égal à $|b|$ et si $b < 0$, pour $u = 0$ et $v = -1$, on obtient $a \times u + b \times v = -b = |b|$ qui est un entier naturel non nul inférieur ou égal à $|b|$.

E est constitué de nombres entiers naturels non nuls. On peut considérer le plus petit de ces entiers naturels non nuls que l'on note n. Montrons que n est un diviseur commun à a et à b puis que n est le PGCD de a et b.

n est un entier naturel tel que $1 \leqslant n \leqslant |b|$. De plus, il existe deux entiers relatifs u_0 et v_0 tels que $n = a \times u_0 + b \times v_0$.

La division euclidienne de $|b|$ par n s'écrit $|b| = qn + r$ où q est un entier naturel et r est un entier naturel tel que $0 \leqslant r < n$. On a alors

$$r = |b| - qn = a \times 0 + b \times \pm 1 - q(au_0 + bv_0) = a(-qu_0) + b(\pm 1 - qv_0).$$

Donc, r est de la forme $a \times u + b \times v$ où u et v sont des entiers relatifs et de plus $0 \leqslant r < n$. Par définition de n, r ne peut pas être strictement positif (car n est le plus petit des entiers strictement positifs de la forme $a \times u + b \times v$ où u et v sont des entiers relatifs). Il ne reste que $r = 0$. Ceci montre que n divise $|b|$.

On montre de la même façon que n divise $|a|$ car $|a|$ est également dans E ($|a| = a \times 1 + b \times 0$ ou $|a| = a \times (-1) + b \times 0$ suivant que a soit positif ou négatif).

Finalement, n est un diviseur commun à a et à b.

Soit maintenant d un diviseur commun à a et à b. D'après le théorème 5, on sait que d divise $a \times u_0 + b \times v_0 = n$. Comme n est un entier naturel non nul, on a en particulier $d \leqslant n$.

Ceci montre que n est le plus grand des diviseurs communs à a et à b ou encore que $n = \text{PGCD}(a,b)$. Par suite, $\text{PGCD}(a,b) = a \times u_0 + b \times v_0$ où u_0 et v_0 sont des entiers relatifs.

2) On a montré au passage que tout diviseur commun à a et b divise le PGCD de a et de b.

Inversement, si d est un diviseur de $n = \text{PGCD}(a,b)$, alors d divise n et n divise a. On en déduit que d divise a d'après le théorème 4. De même, d divise b.

On a montré que les diviseurs communs à a et b sont les diviseurs de leur PGCD.

Théorème 15.
1) Soient a et b deux entiers naturels tels que $a \neq 0$ ou $b \neq 0$. Alors

pour tout entier naturel non nul k, $\text{PGCD}(ka, kb) = k\,\text{PGCD}(a,b)$.

2) Soient a et b deux entiers relatifs tels que $a \neq 0$ ou $b \neq 0$. Alors

pour tout entier relatif non nul k, $\text{PGCD}(ka, kb) = |k|\,\text{PGCD}(a,b)$.

Démonstration. De nouveau, on se contente d'étudier le cas où a, b et k sont des entiers naturels.

Soient a et b deux entiers naturels tels que $a \neq 0$ ou $b \neq 0$. Soit k un entier naturel non nul.
Notons d le PGCD de a et b et d' le PGCD de ka et kb et montrons que $d' = kd$.

• d divise a et b. Donc il existe existe deux entiers naturels q_1 et q_2 tels que $a = q_1 d$ et $b = q_2 d$. Mais alors, $ka = (kq_1)d$ et $kb = (kq_2)d$. Comme kq_1 et kq_2 sont des entiers, on en déduit que kd est un diviseur commun à ka et kb. Puisque d' est le plus grand diviseur commun à a et b, on a en particulier $kd \leqslant d'$.

• k divise ka et kb. Mais alors, d'après le théorème 14, k divise le PGCD de ka et kb qui est d'.
Posons donc $d' = kn$ où n est un entier naturel non nul.

Puisque d' divise ka et kb, il existe des entiers naturels q_1 et q_2 tels que $ka = q_1 d' = q_1 kn$ et $kb = q_2 d' = q_2 kn$. Après simplification par l'entier naturel non nul k, on obtient $a = q_1 n$ et $b = q_2 n$. Par suite, n est un diviseur commun à a et b et donc un diviseur du PGCD de a et b qui est d, toujours d'après le théorème 14. En particulier, $n \leqslant d$ puis $kn \leqslant kd$ ou encore $d' \leqslant kd$.

Finalement, $d' = kd$ ce qu'il fallait démontrer.

---

3) Algorithme d'Euclide

On va maintenant mettre en place un algorithme nous fournissant le PGCD de deux entiers naturels non nuls donnés. Tout démarre avec le résultat suivant :

Théorème 16 (lemme d'Euclide). Soient a et b deux entiers naturels non nuls.
Soit r le reste de la division euclidienne de a par b. Alors

$$\text{PGCD}(a,b) = \text{PGCD}(b,r).$$

Démonstration. Soient a et b deux entiers naturels non nuls. La division euclidienne de a par b s'écrit $a = bq + r$ où q est un entier naturel et r est un entier naturel tel que $0 \leqslant r < b$.

Soit d un entier naturel non nul.

Si d divise a et d divise b, alors d divise $a - bq = r$ d'après le théorème 5. d est alors un diviseur commun à b et r.

Inversement, si d divise b et d divise r, alors d divise $a = bq + r$ d'après le théorème 5. d est alors un diviseur commun à a et b.

En résumé, l'ensemble des diviseurs communs à a et à b est aussi l'ensemble des diviseurs communs à b et à r. En particulier, le plus grand des diviseurs communs à a et b est aussi le plus grand des diviseurs communs à b et r, ce qu'il fallait démontrer.

Exemple. Analysons maintenant comment ce lemme nous permet de déterminer le PGCD de 3780 et 1296.

On commence par effectuer la division euclidienne du plus grand des deux entiers 3780 et 1296 par le plus petit :

$$3780 = 2 \times 1296 + 1188,$$

avec $0 \leqslant 1188 < 1296$. D'après le lemme d'Euclide, le PGCD de 3780 et 1296 est aussi le PGCD de 1296 et 1188. Le problème n'est pas résolu mais il est plus simple à résoudre car les deux entiers 1296 et 1188 sont plus petits que les entiers de départ.

On recommence en effectuant la division euclidienne de 1296 par 1188.

$$1296 = 1 \times 1188 + 108,$$

avec $0 \leqslant 108 < 1296$. le PGCD de 3780 et 1296 est aussi le PGCD de 1296 et 1188 qui lui-même est le PGCD de 1188 et 108. On effectue la division euclidienne de 1188 par 108 :

$$1188 = 11 \times 108 + 0.$$

Cette fois-ci, la division « tombe juste » ou encore l'entier 108 divise l'entier 1188. Le théorème 13 nous permet alors d'affirmer que le PGCD de 1188 et 108 est 108. Finalement

$$\mathrm{PGCD}(3780, 1296) = \mathrm{PGCD}(1296, 1188) = \mathrm{PGCD}(1188, 108) = 108.$$

Le problème a été résolu. ❑

Analysons maintenant le cas général. On se donne deux entiers naturels non nuls a et b où on a appelé a le plus grand des deux entiers a et b et on veut le PGCD de a et b.

Il existe deux entiers naturels q_0 et r_0 tels que $a = b \times q_0 + r_0$ et $0 \leqslant r_0 < b$. Une discussion se présente alors :

- si $r_0 = 0$, alors b divise a et donc $\mathrm{PGCD}(a, b) = b$ d'après le théorème 13.
- si $0 < r_0 < b$, le PGCD de a et b est aussi le PGCD de b et r_0 d'après le théorème 16.

On recommence en effectuant la division euclidienne de b par r_0. Il existe deux entiers naturels q_1 et r_1 tels que $b = q_1 \times r_0 + r_1$ et $0 \leqslant r_1 < r_0$.

- si $r_1 = 0$, alors r_0 divise b et donc $\mathrm{PGCD}(a, b) = \mathrm{PGCD}(b, r_0) = r_0$ d'après les théorèmes 13 et 16.
- si $0 < r_1 < r_0$, le PGCD de a et b est aussi le PGCD de b et r_0 d'après le théorème 16.

On recommence en effectuant la division euclidienne de r_0 par r_1. Il existe deux entiers naturels q_2 et r_2 tels que $r_0 = q_2 \times r_1 + r_2$ et $0 \leqslant r_2 < r_1$.

- si $r_2 = 0$, alors $\mathrm{PGCD}(a, b) = \mathrm{PGCD}(b, r_0) = \mathrm{PGCD}(r_0, r_1) = r_1$.
- si $0 < r_2 < r_1$, on recommence ...

Pour unifier les notations, on pose $r_{-2} = a$ et $r_{-1} = b$. L'algorithme d'Euclide se décrit alors de la manière suivante :

pour tout $k \geqslant -2$, tant que le reste r_{k+1} n'est pas nul,
on effectue la division euclidienne de r_k par r_{k+1} :
$r_k = q_{k+2} r_{k+1} + r_{k+2}$ avec q_{k+2} et r_{k+2} entiers tels que $0 \leqslant r_{k+2} < r_{k+1}$.

Il s'agit maintenant de vérifier que cet algorithme s'arrête ou encore il s'agit de vérifier qu'il existe au moins un reste égal à 0.

Supposons par l'absurde que pour tout entier $k \geqslant -2$, r_k ne soit pas nul. Alors, les entiers r_0, r_1, r_2, ... constituent une suite (r_k) d'entiers **naturels** strictement décroissante. Mais ceci est impossible car une suite d'entiers **relatifs** strictement décroissante finit par prendre une valeur strictement négative puisqu'on perd au moins 1 à chaque étape.

Donc, l'algorithme d'Euclide s'arrête. Si on note r_n le dernier reste non nul dans cet algorithme, par définition r_{n+1} est nul et donc $r_{n-1} = q_{n+1} r_n + r_{n+1} = q_{n+1} r_n$. Par suite, le dernier reste non nul r_n est un diviseur de r_{n-1}. On en déduit que

$$\mathrm{PGCD}(a, b) = \mathrm{PGCD}(b, r_0) = \ldots = \mathrm{PGCD}(r_{n-1}, r_n) = r_n.$$

On a montré que

Le PGCD de a et b est le dernier reste non nul dans l'algorithme d'Euclide.

Exercice 4.
1) Déterminer le PGCD de 12642 et 2382.
2) En déduire les diviseurs communs à 12642 et 2382 qui sont des entiers naturels.

Solution. **1)** L'algorithme d'Euclide appliqué à 12642 et 2382 s'écrit

$$\begin{aligned}
12642 &= 5\times 2382 + 732\\
2382 &= 3\times 732 + 186\\
732 &= 3 \times 186 + 174\\
186 &= 1 \times 174 + 12\\
174 &= 14 \times 12 + 6\\
12 &= 2 \times 6 + 0.
\end{aligned}$$

Le dernier reste non nul est 6 et donc $\text{PGCD}(12642, 2382) = 6$.

2) Les diviseurs communs à 12642 et 2382 sont les diviseurs de leur PGCD à savoir 6.
Les diviseurs communs à 12642 et 2382 qui sont des entiers naturels sont 1, 2, 3 et 6.

IV. Nombres premiers entre eux. Théorème de Bézout *et* Gauss

1) Nombres premiers entre eux

Définition 3. Soient a et b deux entiers relatifs tels que $a \neq 0$ ou $b \neq 0$.
a et b sont **premiers entre eux** si et seulement si $\text{PGCD}(a, b) = 1$.

Par exemple, le PGCD de 4 et 6 est 2 et donc 4 et 6 ne sont pas premiers entre eux.
Par contre, le PGCD de 4 et 5 est 1 et donc 4 et 5 sont premiers entre eux.

Remarque. Quand on prend deux entiers naturels non nuls au hasard, trois situations sont possibles :

Situation 1 : a et b sont premiers entre eux (par exemple $a = 4$ et $b = 5$).
Situation 2 : l'un des deux entiers a ou b divise l'autre (par exemple $a = 4$ et $b = 8$).
Situation 3 : a et b ne sont pas premiers entre eux et aucun des deux entiers a ou b ne divise l'autre (par exemple $a = 4$ et $b = 6$).

Ainsi, la phrase « a et b sont premiers entre eux » n'est pas le contraire de la phrase « a divise b ou b divise a ».

Théorème 17. Soient a et b deux entiers relatifs tels que $a \neq 0$ ou $b \neq 0$. Soit d un entier relatif non nul.
d est PGCD de a et b si et seulement si il existe deux entiers relatifs a' et b' premiers entre eux tels que $a = da'$ et $b = db'$.

Démonstration. Soient a et b deux entiers relatifs tels que $a \neq 0$ ou $b \neq 0$ et soit d un entier relatif non nul.

• S'il existe deux entiers relatifs a' et b' premiers entre eux tels que $a = da'$ et $b = db'$, alors d'après le théorème 15,

$$\text{PGCD}(a, b) = \text{PGCD}(da', db') = d \times \text{PGCD}(a', b') = d \times 1 = d.$$

• Si d est le PGCD de a et b, alors il existe deux entiers relatifs a' et b' tels que $a = da'$ et $b = db'$. De plus,

$$d = \text{PGCD}(a, b) = \text{PGCD}(da', db') = d \times \text{PGCD}(a', b'),$$

et après simplification par l'entier relatif non nul d, on obtient $\text{PGCD}(a', b') = 1$.

---

2) Théorème de Bézout

On donne maintenant un théorème très important en arithmétique qui permet, suivant la situation, de décider si deux entiers sont premiers entre eux ou pas.

Théorème 18 (théorème de Bézout).
Soient a et b deux entiers relatifs tels que $a \neq 0$ ou $b \neq 0$.
a et b sont premiers entre eux si et seulement si il existe deux entiers relatifs u et v tels que $a \times u + b \times v = 1$.

Démonstration. Soient a et b deux entiers relatifs tels que $a \neq 0$ ou $b \neq 0$.

Si $\text{PGCD}(a, b) = 1$, d'après le théorème 14, il existe deux entiers relatifs u et v tels que $a \times u + b \times v = 1$.

Réciproquement, supposons qu'il existe deux entiers relatifs u et v tels que $a \times u + b \times v = 1$.
Soit d entier naturel non nul qui est un diviseur commun à a et à b. Alors, d divise $a \times u + b \times v$ d'après le théorème 5 et donc d divise 1. Puisque d est un entier naturel non nul, on en déduit que $d = 1$.
Ainsi, 1 est le seul diviseur commun à a et b et donc $\text{PGCD}(a, b) = 1$.

On a montré que a et b sont premiers entre eux si et seulement si il existe deux entiers relatifs u et v tels que $a \times u + b \times v = 1$.

Exercice 5. Montrer que pour tout entier naturel n, les entiers naturels n et $n + 1$ sont premiers entre eux.

Solution. Soit n un entier naturel.

$$1 \times (n + 1) + (-1) \times n = 1.$$

Donc, il existe des entiers relatifs u et v tels que $(n+1)\times u + n \times v = 1$. D'après le théorème de Bézout, les entiers n et $n+1$ sont premiers entre eux.

Ainsi, deux entiers consécutifs sont toujours premiers entre eux. ❑

Le théorème suivant est une application du théorème de Bézout.

Théorème 19.
Soient a, b et c trois entiers relatifs non nuls.
Si c est premier avec a et b alors c est premier avec $a \times b$.

Démonstration. Soient a, b et c trois entiers relatifs non nuls.

Supposons que c soit premier avec a et b. D'après le théorème de Bézout, il existe quatre entiers relatifs u_1, v_1, u_2 et v_2 tels que $au_1 + cv_1 = 1$ et $bu_2 + cv_2 = 1$.

En multipliant membre à membre ces deux égalités, on obtient

$$abu_1u_2 + acu_1v_2 + bcv_1u_2 + c^2v_1v_2 = 1$$

ou encore

$$abu_1u_2 + c(au_1v_2 + bv_1u_2 + cv_1v_2) = 1.$$

Puisque u_1u_2 et $au_1v_2 + bv_1u_2 + cv_1v_2$ sont des entiers relatifs, le théorème de Bézout permet d'affirmer que les entiers c et ab sont premiers entre eux.

---

3) Théorème de Gauss

On énonce maintenant un autre théorème très important de l'arithmétique qui est une conséquence du théorème de Bézout.

Théorème 20 (théorème de Gauss).
Soient a, b et c trois entiers relatifs tels que $a \neq 0$.
Si a divise $b \times c$ et si a est premier à b, alors a divise c.

Démonstration. Soient a, b et c trois entiers relatifs tels que $a \neq 0$, a divise $b \times c$ et a est premier à b.

• Puisque a divise bc, il existe un entier relatif q tel que $bc = qa$ (I).
• Puisque a est premier à b, il existe deux entiers relatifs u et v tels que $au + bv = 1$ (II) d'après le théorème de Bézout.

On multiplie par c les deux membres de l'égalité (II) puis on obtient grâce à l'égalité (I) :

$$c = acu + bcv = acu + qav = a(cu + qv).$$

Puisque $cu + qv$ est un entier relatif, on a montré que a divise c.

L'hypothèse « a est premier à b » est essentielle. Par exemple, l'entier 6 divise l'entier $4 \times 9 = 36$ mais l'entier 6 ne divise ni l'entier 4, ni l'entier 9.

4) Résolution de l'équation $ax + by = c$

On se donne trois entiers relatifs a, b et c tels que $a \neq 0$ ou $b \neq 0$. On cherche tous les couples (x, y) d'entiers relatifs tels que

$$ax + by = c \qquad (E).$$

Nous donnerons au cours de de paragraphe quelques généralités sur cette équation, mais nous décrirons sa résolution à travers des exemples qui serviront de modèle.

La résolution s'effectue en deux étapes :

1) on détermine une solution particulière de l'équation (E)
2) on détermine toutes les solutions en fonction de cette solution particulière.

a) Recherche d'une solution particulière de l'équation $ax + by = c$

Commençons par voir à travers trois exemples comment obtenir une solution particulière de (E).

Exemple 1. Considérons l'équation

$$5x + 2y = 1 \qquad (E)$$

Dans ce premier exemple, on devine une solution particulière : le couple $(x_0, y_0) = (1, -2)$ est une solution de l'équation (E) car $5 \times 1 + 2 \times (-2) = 1$.

Exemple 2. Considérons l'équation

$$5x + 2y = 2 \qquad (E)$$

Dans le premier exemple, nous avions deviné que $5 \times 1 + 2 \times (-2) = 1$. En multipliant par 2 les deux membres de cette égalité par 2, on obtient $5 \times 2 + 2 \times (-4) = 2$. Donc, le couple $(x_0, y_0) = (2, -4)$ est une solution particulière de l'équation $5x + 2y = 2$.
De manière générale, si on a trouvé une solution particulière (x_0, y_0) de l'équation $ax + by = 1$, alors $ax_0 + by_0 = 1$ puis $acx_0 + bcy_0 = c$ et donc le couple (cx_0, cy_0) est une solution particulière de l'équation $ax + by = c$.

Exemple 3. Considérons l'équation

$$63x + 55y = 1 \qquad (E)$$

Une solution particulière ne « saute plus aux yeux ». On va voir qu'on en obtient une de manière imparable grâce à l'algorithme d'Euclide.

$$\begin{aligned} 63 &= 1 \times 55 + 8 \\ 55 &= 6 \times 8 + 7 \\ 8 &= 1 \times 7 + 1 \\ (7 &= 7 \times 1 + 0) \end{aligned}$$

Le dernier reste non nul est 1 et donc $PGCD(63, 55) = 1$. Le théorème de Bézout permet d'affirmer que l'équation (E) admet au moins un couple d'entiers relatifs (x_0, y_0) solution.

Nous allons obtenir une telle solution en « remontant » dans l'algorithme. On exprime 1 en fonction de 7 et 8 à partir de la dernière égalité :

$$1 = 8 - 7.$$

On exprime ensuite 7 en fonction de 8 et 55 et donc 1 en fonction de 8 et 55 à partir de l'égalité précédente :

$$\begin{aligned} 1 &= 8 - 7 \\ &= 8 - (55 - 6 \times 8) = 7 \times 8 - 55. \end{aligned}$$

On exprime enfin 8 en fonction de 55 et 63 et donc 1 en fonction de 55 et 63 à partir de la première égalité :

$$\begin{aligned} 1 &= 8 - 7 \\ &= 8 - (55 - 6 \times 8) = 7 \times 8 - 55 \\ &= 7 \times (63 - 55) - 55 = 7 \times 63 - 8 \times 55 = 63 \times 7 + 55 \times (-8). \end{aligned}$$

Le couple $(x_0, y_0) = (7, -8)$ est un couple solution de l'équation $63x + 55y = 1$.

b) Résolution de l'équation $ax + by = c$

Maintenant, que nous avons vu comment obtenir une solution particulière de l'équation (E), passons à la résolution générale de cette équation. Pour cela, nous reprenons l'équation de l'exemple 1 :

$$5x + 2y = 1.$$

On rappelle que le couple $(x_0, y_0) = (1, -2)$ est une solution de cette équation et qu'une conséquence est le fait que les entiers 5 et 2 soient premiers entre eux.

Soit (x, y) un couple d'entiers relatifs.

$$5x + 2y = 2 \Leftrightarrow 5x + 2y = 5x_0 + 2y_0 \Leftrightarrow 5(x - x_0) = 2(y_0 - y).$$

Si (x, y) est un couple d'entiers relatifs solution de (E), alors l'entier 2 divise l'entier $2(y_0 - y)$ qui est égal à l'entier $5(x - x_0)$. Par suite, l'entier 2 divise l'entier $5(x - x_0)$. D'autre part, 2 est premier à 5 et le théorème de Gauss permet d'affirmer que l'entier 2 divise l'entier $x - x_0$.
Par suite, il existe un entier relatif k tel que $x - x_0 = 2k$ ou encore $x = x_0 + 2k$.
De même, l'entier 5 divise $y_0 - y$ et donc il existe un entier relatif k' tel que $y_0 - y = 5k'$ ou encore $y = y_0 - 5k'$.

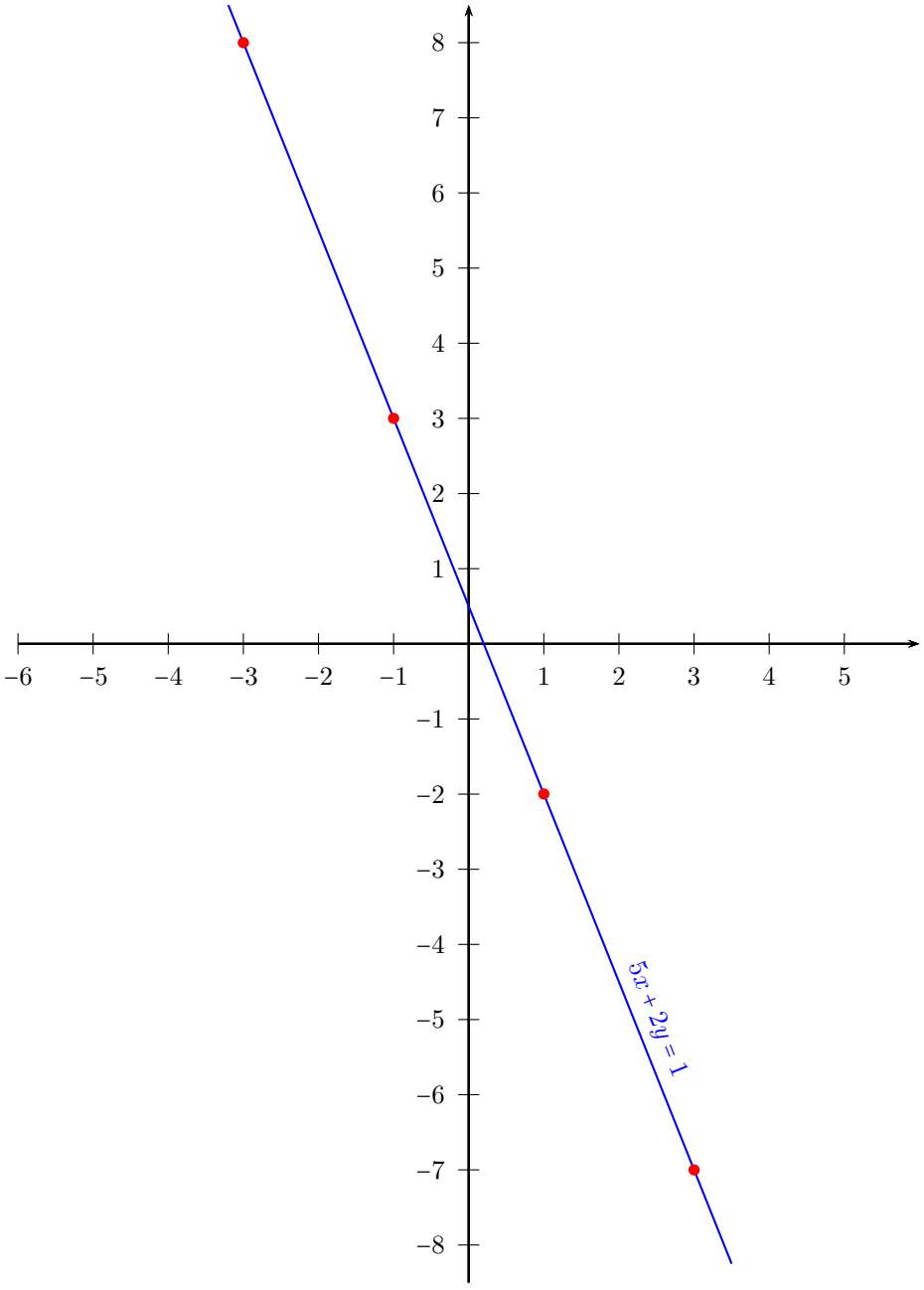
En résumé, **si** (x, y) est un couple d'entiers relatifs solution de l'équation (E), **alors** il existe deux entiers relatifs k et k' tels que $x = x_0 + 2k$ et $y = y_0 - 5k'$.

Soient donc k et k' deux entiers relatifs puis $x = x_0 + 2k$ et $y = y_0 - 5k'$.

$$\begin{aligned} 5x+2y=1 &\Leftrightarrow 5(x_0+2k)+2(y_0-5k')=1 \Leftrightarrow 5x_0+2y_0+10(k-k')=1\\ &\Leftrightarrow 10(k-k')=0 \text{ (car } 5x_0+2y_0=1)\\ &\Leftrightarrow k=k'. \end{aligned}$$

Ainsi, les couples d'entiers relatifs solutions de l'équation (E) sont les couples de la forme $(1+2k,-2-5k)$ où k est un entier relatif. L'équation est résolue.

Interprétons graphiquement le résultat obtenu. Le plan est rapporté à un repère orthonormé $\left(O,\vec{i},\vec{j}\right)$.
L'ensemble des couples (x,y) de **réels** tels que $5x+2y=1$ est une droite que l'on note $(\mathscr{D})$. En déterminant les couples (x,y) d'entiers relatifs tels que $5x+2y=1$, nous avons déterminés les points de $(\mathscr{D})$ à **coordonnées entières**. Par exemple, pour $k\in\{-2;-1;0;1\}$, on obtient les points de coordonnées respectives $(-3,8)$, $(-1,3)$, $(1,-2)$ et $(3,-7)$.



Enonçons maintenant quelques généralités sur l'équation $ax+by=c$. Notons d le PGCD de a et b.
Alors, pour tout couple d'entiers relatifs (x,y), d divise $ax+by$. Par suite, si c n'est pas divisible par d, il n'existe pas de couple d'entiers relatifs (x,y) tel que $ax+by=c$ ou encore l'équation (E) n'a pas de solution (qui soit un couple d'entiers relatif). C'est le cas par exemple pour l'équation $2x+4y=3$.

Supposons maintenant que d divise c. On peut poser $a=da'$, $b=db'$ et $c=dc'$ où a', b' et c' sont trois entiers relatifs et a' et b' sont premiers entre eux (d'après le théorème 17). L'équation (E) s'écrit alors

$$a'x+b'y=c',$$

où cette fois-ci les entiers relatifs a' et b' sont premiers entre eux.

Le théorème de BÉZOUT assure l'existence d'un couple (u_0, v_0) d'entiers relatifs tel que $a'u_0 + b'v_0 = 1$.
En multipliant les deux membres de cette égalité par c, on obtient $a'(cu_0) + b'(cv_0) = c$ et donc le couple $(x_0, y_0) = (cu_0, cv_0)$ est un couple d'entiers relatifs solution de l'équation $a'x + b'y = c'$ et donc de l'équation $ax + by = c$.

En résumé, on peut énoncer :

l'équation (E) a des solutions (dans $\mathbb{Z}$) si et seulement si le PGCD de a et b divise c.

V. Nombres premiers

Dans cette section, « diviseur » signifiera « diviseur entier naturel ».

1) Définition des nombres premiers

Tout nombre entier supérieur ou égal à 2 admet au moins deux diviseurs distincts entiers naturels, à savoir 1 et lui-même. Parmi ces entiers, ceux qui en admettent exactement deux sont les **nombres premiers** :

Définition 4. Soit n un entier naturel supérieur ou égal à 2.
n est **premier** si et seulement si n admet exactement deux diviseurs à savoir 1 et n.

Les premiers nombres premiers sont

2 3 5 7 11 13 17 19 23 ...

Remarque. On peut noter que la liste des nombres premiers commence à 2 et donc que 1 n'est pas un nombre premier. Pourquoi a-t-on choisi de ne pas mettre 1 dans la liste des nombres premiers ?
On verra plus loin que tout nombre entier supérieur ou égal à 2 « se décompose de manière unique en produit de facteurs premiers ». Cela signifie que si $2^a \times 3^b = 2^3 \times 3^2$, alors nécessairement $a = 3$ et $b = 2$ ou aussi que, sans faire de calcul ; on sait que $2^7 \times 3^6 \neq 2^6 \times 3^7$ car les exposants ne sont pas les mêmes. Ceci serait faux si 1 était un nombre premier car $1^2 \times 2^3 = 1^5 \times 2^3$. Pour cette raison, on décide que 1 n'est pas un nombre premier. ❏

On décrit maintenant les nombres supérieur ou égaux à 2 qui ne sont pas des nombres premiers. Ils sont dits **composés**. On peut en donner plusieurs définitions équivalentes :

Définition 5. Soit n un entier naturel supérieur ou égal à 2.
1) n est **composé** si et seulement si n n'est pas premier.
2) n est **composé** si et seulement si n admet au moins un diviseur distinct de 1 et n.
3) n est **composé** si et seulement si il existe deux entiers a et b tels que $n = a \times b$ et $1 < a < n$ et $1 < b < n$.

Par exemple, 6 est composé car $6 = 2 \times 3$ avec $1 < 2 < 6$ et $1 < 3 < 6$.

Théorème 21. Soit n un entier naturel supérieur ou égal à 2.
n admet au moins un diviseur qui est un nombre premier.

Démonstration. Soit $n \geqslant 2$.

• Si n est un nombre premier, alors il admet au moins un diviseur qui est un nombre premier.

• Si n n'est pas premier, n admet au moins un diviseur compris au sens large entre 2 et $n - 1$.

Notons alors p le plus petit des diviseurs de n compris au sens large entre 2 et $n - 1$.
Supposons par l'absurde que p est composé. p admet un diviseur d tel que $2 \leqslant d < p$.
Puisque d divise p et que p divise n, d est un diviseur de n.
Puisque $2 \leqslant d < p \leqslant n - 1$, on a $2 \leqslant d \leqslant n - 1$ et aussi $d < p$.
Ceci contredit le fait que p est le plus petit des diviseurs de n compris au sens large entre 2 et $n - 1$.

Donc p est un nombre premier, diviseur de n.

Dans tous les cas, on a montré que n admet au moins un diviseur qui est un nombre premier.

---

2) Tester si un nombre est premier

A priori, pour tester si un nombre n est premier ou pas, on doit tester si ce nombre est divisible par l'un des entiers k tels que $1 < k < n$. Par exemple,

$\frac{29}{2} = 14,5$. Donc 29 n'est pas divisible par 2.
$\frac{29}{3} = 9,6\ldots$ Donc 29 n'est pas divisible par 3.
$\frac{29}{4} = 7,25$ Donc 29 n'est pas divisible par 4.
$\frac{29}{5} = 5,8$ Donc 29 n'est pas divisible par 5.
$\frac{29}{6} = 4,8\ldots$ Donc 29 n'est pas divisible par 6.
$\frac{29}{7} = 4,1\ldots$ Donc 29 n'est pas divisible par 7.
$\frac{29}{8} = 3,625$ Donc 29 n'est pas divisible par 8.
$\frac{29}{9} = 3,2\ldots$ Donc 29 n'est pas divisible par 9.
$\frac{29}{10} = 2,9$ Donc 29 n'est pas divisible par 10.
$\frac{29}{11} = 2,6\ldots$ Donc 29 n'est pas divisible par 11.
$\frac{29}{12} = 2,4\ldots$ Donc 29 n'est pas divisible par 12.
$\frac{29}{13} = 2,2\ldots$ Donc 29 n'est pas divisible par 13.
$\frac{29}{14} = 2,07\ldots$ Donc 29 n'est pas divisible par 14.
$\frac{29}{15} = 1,9\ldots$ Donc 29 n'est pas divisible par 15.
$\frac{29}{16} = 1,8125$ Donc 29 n'est pas divisible par 16.
$\frac{29}{17} = 1,7\ldots$ Donc 29 n'est pas divisible par 17.
$\frac{29}{18} = 1,6\ldots$ Donc 29 n'est pas divisible par 18.
$\frac{29}{19} = 1,5\ldots$ Donc 29 n'est pas divisible par 19.
$\frac{29}{20} = 1,45$ Donc 29 n'est pas divisible par 20.
$\frac{29}{21} = 1,3\ldots$ Donc 29 n'est pas divisible par 21.
$\frac{29}{22} = 1,3\ldots$ Donc 29 n'est pas divisible par 22.
$\frac{29}{23} = 1,2\ldots$ Donc 29 n'est pas divisible par 23.
$\frac{29}{24} = 1,2\ldots$ Donc 29 n'est pas divisible par 24.
$\frac{29}{25} = 1,1\ldots$ Donc 29 n'est pas divisible par 25.
$\frac{29}{26} = 1,1\ldots$ Donc 29 n'est pas divisible par 26.
$\frac{29}{27} = 1,07\ldots$ Donc 29 n'est pas divisible par 27.
$\frac{29}{28} = 1,03\ldots$ Donc 29 n'est pas divisible par 28.

Puisque 29 n'est divisible par aucun des entiers compris au sens large entre 2 et 28, 29 est un nombre premier. Un premier commentaire : c'est très long et nous vous laissons le soin de tester par cette méthode si oui ou non 1231 est premier.

Nous allons essayer de diminuer le nombre de calculs. Par exemple, nous avons testé si 29 était divisible par 2 ou encore nous avons testé si 29 était un multiple de 2. Il n'était alors plus la peine de tester si 29 était un multiple de 4 ou 6 ou 8 . . . car un multiple de 4 est d'abord un multiple de 2. Nous avons donc fait beaucoup de calculs superflus. Cette constatation divise déjà par deux le nombre de vérification à effectuer :

$\frac{29}{2} = 14,5$. Donc 29 n'est pas divisible par 2.
$\frac{29}{3} = 9,6\ldots$ Donc 29 n'est pas divisible par 3.
$\frac{29}{5} = 5,8$ Donc 29 n'est pas divisible par 5.
$\frac{29}{7} = 4,1\ldots$ Donc 29 n'est pas divisible par 7.
$\frac{29}{9} = 3,2\ldots$ Donc 29 n'est pas divisible par 9.
$\frac{29}{11} = 2,6\ldots$ Donc 29 n'est pas divisible par 11.
$\frac{29}{13} = 2,2\ldots$ Donc 29 n'est pas divisible par 13.
$\frac{29}{15} = 1,9\ldots$ Donc 29 n'est pas divisible par 15.
$\frac{29}{17} = 1,7\ldots$ Donc 29 n'est pas divisible par 17.
$\frac{29}{19} = 1,5\ldots$ Donc 29 n'est pas divisible par 19.
$\frac{29}{21} = 1,3\ldots$ Donc 29 n'est pas divisible par 21.
$\frac{29}{23} = 1,2\ldots$ Donc 29 n'est pas divisible par 23.
$\frac{29}{25} = 1,1\ldots$ Donc 29 n'est pas divisible par 25.
$\frac{29}{27} = 1,07\ldots$ Donc 29 n'est pas divisible par 27 et donc 29 est premier.

De manière générale, quand nous avons vérifié que 29 n'était pas divisible par un certain entier k, ce n'était plus la peine de tester si 29 était divisible par $2k$, $3k$, ... Dit autrement, il n'était pas la peine de tester si oui ou non, 29 était divisible par un nombre composé :

$\frac{29}{2} = 14,5$. Donc 29 n'est pas divisible par 2.
$\frac{29}{3} = 9,6\ldots$ Donc 29 n'est pas divisible par 3.
$\frac{29}{5} = 5,8$ Donc 29 n'est pas divisible par 5.
$\frac{29}{7} = 4,1\ldots$ Donc 29 n'est pas divisible par 7.
$\frac{29}{11} = 2,6\ldots$ Donc 29 n'est pas divisible par 11.
$\frac{29}{13} = 2,2\ldots$ Donc 29 n'est pas divisible par 13.
$\frac{29}{17} = 1,7\ldots$ Donc 29 n'est pas divisible par 17.
$\frac{29}{19} = 1,5\ldots$ Donc 29 n'est pas divisible par 19.
$\frac{29}{23} = 1,2\ldots$ Donc 29 n'est pas divisible par 23 et donc 29 est premier.

Le nombre de tests est passé de 27 à 9. On va encore diminuer le nombre de ces tests.

Théorème 22. Soit n un entier naturel supérieur ou égal à 4.
n est composé si et seulement si n est divisible par l'un des entiers k tels que $2 \leqslant k \leqslant \sqrt{n}$.

Démonstration. Soit n un entier naturel supérieur ou égal à 4. Alors $\sqrt{n} \geqslant 2$.

• Supposons que n soit composé. Il existe deux entiers a et b tels que $n = a \times b$ et $1 < a < n$ et $1 < b < n$.
Supposons par l'absurde que $a > \sqrt{n}$ et $b > \sqrt{n}$. En multipliant membre à membre ces inégalités, on obtient $ab > n$ et en particulier $ab \neq n$. Ceci contredit le fait que $ab = n$ et donc l'un au moins des deux entiers a ou b est inférieur ou égal à $\sqrt{n}$. Comme d'autre part les deux entiers a et b sont strictement supérieurs à 1 ou encore sont supérieurs ou égaux à 2, on vient de trouver un diviseur k de n vérifiant $2 \leqslant k \leqslant \sqrt{n}$.

• Supposons que n soit divisible par l'un des entiers k tels que $2 \leqslant k \leqslant \sqrt{n}$.
Puisque $n \geqslant 4$, on a $n > \sqrt{n}$ car $n^2 - \left(\sqrt{n}\right)^2 = n^2 - n = n(n-1) > 0$. Donc l'entier k vérifie $1 < k < n$.

Puisque n admet un diviseur k tel que $1 < k < n$, n est composé.

Quand nous avons testé, si oui ou non 29 était premier, il n'était donc pas la peine de vérifier si 29 était divisible par des nombres strictement supérieurs à sa racine carrée. Puisque $\sqrt{29} = 5,3\ldots$, les vérifications suivantes suffisaient pour montrer que 29 est premier :

$\frac{29}{2} = 14,5$. Donc 29 n'est pas divisible par 2.
$\frac{29}{3} = 9,6\ldots$ Donc 29 n'est pas divisible par 3.
$\frac{29}{5} = 5,8$ Donc 29 n'est pas divisible par 5 et donc 29 est premier.

On peut alors énoncer le résultat définitif suivant :

Théorème 23. Soit n un entier naturel supérieur ou égal à 4.
n est composé si et seulement si n est divisible par l'un des nombres premiers p tels que $p \leqslant \sqrt{n}$.
n est premier si et seulement si n n'est divisible par aucun des nombres premiers inférieurs ou égaux à $\sqrt{n}$.

Démonstration. Soit $n \geqslant 4$. Montrons que n est composé si et seulement si n est divisible par l'un des nombres premiers p tels que $2 \leqslant p \leqslant \sqrt{n}$.

• Si n est divisible par l'un des nombres premiers p tels que $2 \leqslant p \leqslant \sqrt{n}$, d'après le théorème 21, n est composé.

• Si n est composé, d'après le théorème 21, n admet au moins un diviseur k tel que $2 \leqslant k \leqslant \sqrt{n}$.
D'après le théorème 21, l'entier k admet au moins un diviseur p qui est un nombre premier.
Le nombre premier p divise l'entier k et donc $2 \leqslant p \leqslant k \leqslant \sqrt{n}$. D'autre part, p divise k et$k$ divise n et donc p divise n d'après le théorème 4.

On a montré que n admet un diviseur premier p tel que $2 \leqslant p \leqslant \sqrt{n}$.

Exercice 6. Démontrer que 331 est un nombre premier.

Solution. $\sqrt{331} = 18,\ldots$ Les nombres premiers inférieurs ou égaux à $\sqrt{331}$ sont 2, 3, 5, 7, 11, 13 et 17.
$\frac{331}{2} = 165,5$ et donc 331 n'est pas divisible par 2.
$\frac{331}{3} = 110,3\ldots$ et donc 331 n'est pas divisible par 3.
$\frac{331}{5} = 66,2$ et donc 331 n'est pas divisible par 5.
$\frac{331}{7} = 47,2\ldots$ et donc 331 n'est pas divisible par 7.
$\frac{331}{11} = 30,09\ldots$ et donc 331 n'est pas divisible par 11.
$\frac{331}{13} = 25,4\ldots$ et donc 331 n'est pas divisible par 13.
$\frac{331}{17} = 19,47\ldots$ et donc 331 n'est pas divisible par 17.
Finalement, 331 n'est divisible par aucun nombre premier inférieur ou égal à sa racine et donc 331 est un nombre premier.

---

3) Le crible d'Erathostène

On va maintenant dresser la liste des nombres premiers compris entre 1 et 100 par exemple, en effectuant un minimum de calcul. Pour cela, on commence par placer les entiers compris entre 1 et 100 dans un tableau à 10 lignes et 10 colonnes. On barre tout de suite 1 qui n'est pas premier.

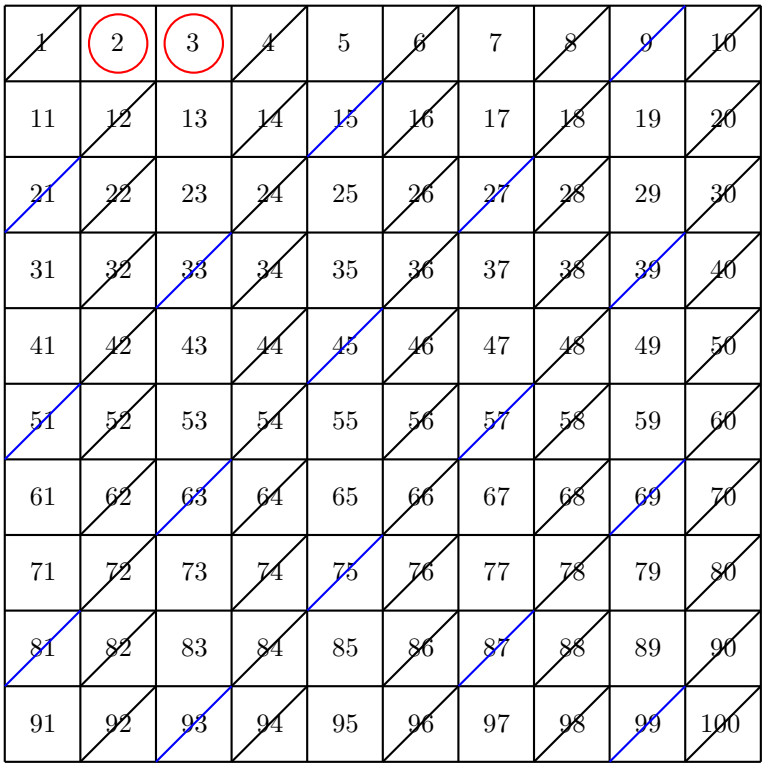
1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

D'après le paragraphe précédent, si un nombre compris entre 1 et 100 n'est pas premier, il admet au moins un diviseur premier compris entre 2 et $\sqrt{100} = 10$ et dans le cas contraire, ce nombre est premier.
Pour avoir tous les nombres premiers inférieurs ou égaux à 100, il suffit de connaître tous les nombres premiers inférieurs ou égaux à 10 et de barrer leurs multiples stricts. Les nombres non barrés seront les nombres premiers cherchés. On procède de façon algorithmique.

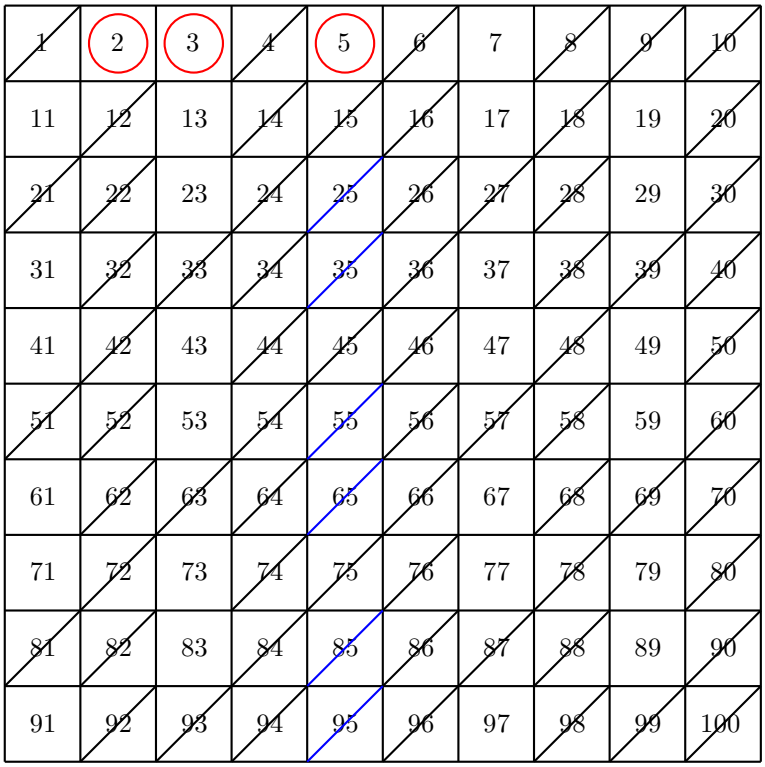
On entoure 2 qui est premier puis on barre tous les multiples de 2 sauf 2.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Le premier entier non barré après 2 est 3. 3 n'est donc multiple d'aucun nombre premier le précédant et par suite, 3 est premier. On entoure 3 puis on barre tous les multiples de 3 sauf 3 qui n'ont pas encore été barrés.



Le premier entier non barré après 3 est 5. 5 n'est donc multiple d'aucun nombre premier le précédant et par suite, 5 est premier. On entoure 5 puis on barre tous les multiples de 5 sauf 5 qui n'ont pas encore été barrés.



Le premier entier non barré après 5 est 7. 7 est premier. On entoure 7 puis on barre tous les multiples de 7 sauf 7 qui n'ont pas encore été barrés.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

D'après la remarque initiale, c'est fini. Les nombres non barrés sont les nombres premiers inférieurs ou égaux à 100.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Les nombres premiers inférieurs ou égaux à 100 sont

2 3 5 7 11 13 17 19 23 29 31 37 41
43 47 53 59 61 67 71 73 79 83 89 97

4) Quelques propriétés des nombres premiers

On énonce maintenant quelques résultats fournissant des raisonnements de base sur les nombres premiers.

Théorème 24. Soient n un entier naturel non nul et p un nombre premier.
Le PGCD de n et p est 1 ou p.
Plus précisément, si p divise n, $\text{PGCD}(n,p) = p$ et si p ne divise pas n, $\text{PGCD}(n,p) = 1$.

Démonstration. Soient n un entier naturel non nul et p un nombre premier. Soit $d = \text{PGCD}(n,p)$.

d est en particulier un diviseur de p et donc $d = 1$ ou $d = p$.
Si p divise n, alors le plus grand diviseur commun à p et n est p. Donc, $d = p$.
Si d ne divise pas n, on ne donc peut avoir $d = p$ et il reste $d = 1$.

Commentaire. Ce résultat est faux si p n'est pas premier. Par exemple, le PGCD de 6 et 4 est 2 et n'est ni 1, ni 4.

Une conséquence immédiate est le théorème suivant :

Théorème 25. Deux nombres premiers distincts sont premiers entre eux.

Théorème 26. Soit p un entier naturel supérieur ou égal à 3.
p est premier si et seulement si p est premier à tous les entiers naturels k tels que $2 \leqslant k \leqslant p-1$.

Démonstration. Soit p un entier naturel supérieur ou égal à 3.
p est premier si et seulement si p n'est divisible par aucun des entiers k tels que $2 \leqslant k \leqslant p-1$.
D'après le théorème 24, cette dernière phrase est équivalente au fait que p est premier à tous les entiers naturels k tels que $2 \leqslant k \leqslant p-1$.

Théorème 27. Soient p un nombre premier et a et b des entiers naturels non nuls.
Si p divise $a \times b$, alors p divise a ou p divise b.

Démonstration. Soient p un nombre premier et a et b des entiers naturels non nuls tels que p divise $a \times b$.

Supposons que p ne divise pas a. Alors, d'après le théorème 23, p est premier à a.

Ainsi, p divise $a \times b$ et est premier à a. Mais alors, d'après le théorème de Gauss, p divise b.

Commentaire. Ce résultat est faux si p n'est pas premier. Par exemple, l'entier 6 divise $3 \times 8 = 24$ mais 6 ne divise pas 3 et 6 ne divise 8.

5) Infinité de l'ensemble des nombres premiers

Il existe une infinité de nombres premiers mais ceci n'est pas immédiat et doit être démontré :

Théorème 28. Il existe une infinité de nombres premiers deux à deux distincts.

Démonstration. Montrons par récurrence que pour tout entier naturel non nul n il existe n nombres premiers deux à deux distincts.

• Le nombre 2 est premier. L'affirmation est donc vraie quand $n = 1$.

• Soit $n \geqslant 1$. Supposons qu'il existe n nombres premiers deux à deux distincts. Notons les $p_1, \ldots, p_n$.
Montrons alors qu'il existe $n+1$ nombres premiers deux à deux distincts.

Soit $a = p_1 \times \ldots \times p_n + 1$. Soit k un entier naturel tel que $1 \leqslant k \leqslant n$.
Si $n \geqslant 2$, on note P le produit des nombres premiers p_i où $1 \leqslant i \leqslant n$ et $i \neq k$ et si $n = 1$, on pose $P = 1$.
Dans tous les cas, P est une entier naturel tel que $a = p_k \times P + 1$. Cette dernière égalité s'écrit encore

$$1 \times a + (-P) \times p_k = 1,$$

où $u = 1$ et $v = -P$ sont des entiers relatifs. D'après le théorème de Bézout, les entiers a et p_k sont premiers entre eux.

D'autre part, l'entier a est supérieur ou égal à 2 car $a \geqslant p_1 + 1 \geqslant 2 + 1 \geqslant 2$. D'après le théorème 21, a admet au moins un diviseur premier que l'on note p.
Si p est l'un des nombres premiers p_k où $1 \leqslant k \leqslant n$, alors p divise a et p divise p_k. p est donc un diviseur commun à a et p_k distinct de 1. Ceci contredit le fait que a et p_k sont premiers entre eux.

Donc, p est un nombre premier distinct de chacun des nombres premiers $p_1, \ldots, p_n$. Il existe donc $n+1$ nombres premiers deux à deux distincts.

Le résultat est démontré par récurrence.

---

6) Décomposition en produit de facteurs premiers

On énonce maintenant le théorème fondamental de l'arithmétique :

Théorème 29 (le théorème fondamental de l'arithmétique).
Soit n un entier naturel supérieur ou égal à 2.
1) n se décompose en produit de nombres premiers ou encore n peut s'écrire sous la forme

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_k^{\alpha_k},$$

où les nombres $p_1, \ldots, p_k$ sont des nombres premiers deux à deux distincts et les exposants $\alpha_1, \ldots, \alpha_k$ sont des entiers naturels non nuls.
2) La décomposition est unique à l'ordre près des facteurs.

Commentaire. Il est sous-entendu que, dans l'égalité $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_k^{\alpha_k}$, on peut avoir $k = 1$ ou encore il peut n'apparaître qu'un seul nombre premier p_1. Si de plus $\alpha_1 = 1$, alors $n = p_1$ et on pourra dire conventionnellement que n est un produit de 1 facteur premier. ❑

On admet le théorème 29 même si l'existence de la décomposition peut être assez facilement établie grâce au théorème 21.

Définition 6. Soit n un entier naturel supérieur ou égal à 2.
L'écriture $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_k^{\alpha_k}$ où les nombres premiers p_i sont deux à deux distincts et les exposants α_i sont des entiers naturels non nuls s'appelle la **décomposition primaire de** n.

Exemple. La décomposition explicite d'un entier supérieur ou égal à 2 peut s'effectuer méthodiquement comme dans l'exemple ci-dessous.

Par exemple, déterminons la décomposition primaire de 47432. Le premier nombre premier est 2 et 47432 est pair. On commence par récupérer la plus grande puissance de 2 divisant 47432 :

$$\begin{aligned} 47432 &= 2 \times 23716 \\ &= 2 \times 2 \times 11858 \\ &= 2 \times 2 \times 2 \times 5929. \end{aligned}$$

5929 est impair et donc n'est plus divisible par 2.
On passe alors au nombre premier suivant qui est 3. $\dfrac{5929}{3} = 1976,3\ldots$ et donc 5929 n'est pas divisible par 3.
On passe au nombre premier suivant qui est 5. $\dfrac{5929}{5} = 1185,8$ et donc 5929 n'est pas divisible par 5.
On passe au nombre premier suivant qui est 7. $\dfrac{5929}{7} = 847$. On peut poursuivre.

$$\begin{aligned} 47432 &= 2^3 \times 5929 \\ &= 2^3 \times 7 \times 847 \\ &= 2^3 \times 7 \times 7 \times 121. \end{aligned}$$

Comme $\dfrac{121}{7} = 17,2\ldots$, 121 n'est plus divisible par 7. On passe au nombre premier suivant qui est 11 et on obtient :

$$47432 = 2^3 \times 7^2 \times 11^2.$$

Puisque 2, 7 et 11 sont des nombres premiers, la décomposition est achevée. ❑

On donne maintenant trois applications du théorème fondamental de l'arithmétique.

Théorème 30. Soient n et m deux entiers naturels supérieurs ou égaux à 2.
n et m sont premiers entre eux si et seulement si n et m n'ont pas de facteur premier commun.

Démonstration. Soient n et m deux entiers naturels supérieurs ou égaux à 2. Soit d le PGCD de n et m.

Si m et n ont un facteur premier p commun, p est un diviseur commun à n et m et donc p un diviseur de d d'après le théorème 14. Puisque p est supérieur ou égal à 2, on en déduit que d n'est pas égal à 1 et donc que n et m ne sont pas premiers entre eux.

Si m et n ne sont pas premier entre eux, d est supérieur ou égal à 2 et et donc divisible par au moins un nombre premier p. Puisque p divise d et que d divise n et m, on en déduit que p est un diviseur commun à n et m.

On a montré que n et m ne sont pas premiers entre eux si et seulement si n et m ont un facteur premier commun ou encore n et m sont premiers entre eux si et seulement si n et m n'ont pas de facteur premier commun.

Théorème 31. Soit n un entier naturel supérieur ou égal à 2.
On suppose connue la décomposition primaire de n :

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_k^{\alpha_k},$$

où les nombres $p_1, \ldots, p_k$ sont des nombres premiers deux à deux distincts et les exposants $\alpha_1, \ldots, \alpha_k$ sont des entiers naturels non nuls.

1) Les diviseurs de n sont les entiers de la forme :

$$p_1^{\beta_1} \times p_2^{\beta_2} \times \ldots \times p_k^{\beta_k},$$

où $\beta_1, \ldots, \beta_k$ sont des entiers naturels tels que $0 \leqslant \beta_1 \leqslant \alpha_1, \ldots, 0 \leqslant \beta_k \leqslant \alpha_k$.

2) Le nombre de diviseurs de n est $(\alpha_1 + 1) \times \ldots \times (\alpha_k + 1)$.

Démonstration. 1) $1 = p_1^0 \times \ldots \times p_k^0$ est un diviseur de n.
Soit d un diviseur de n tel que $d \geqslant 2$. Soit p un facteur premier de d.
p divise d et d divise n. Donc p divise n ou encore p est l'un des nombres premiers $p_1, \ldots, p_k$. On peut donc poser

$$d = p_1^{\beta_1} \times p_2^{\beta_2} \times \ldots \times p_k^{\beta_k}$$

où $\beta_1, \ldots, \beta_k$ sont des entiers naturels.

Soit i un entier naturel tel que $1 \leqslant i \leqslant k$. $p_i^{\beta_i}$ divise d et donc $p_i^{\beta_i}$ divise n ou encore $p_i^{\beta_i}$ divise $p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_k^{\alpha_k}$. $p_i^{\beta_i}$ est premier avec le produit des $p_j^{\alpha_j}$ où $j \neq i$ car n'a pas de facteur premier commun avec ce produit. D'après le théorème de Gauss, $p_i^{\beta_i}$ divise $p_i^{\alpha_i}$. Ceci impose $\beta_i \leqslant \alpha_i$.

Ainsi, un diviseur de n est un entier naturel de la forme $d = p_1^{\beta_1} \times p_2^{\beta_2} \times \ldots \times p_k^{\beta_k}$, où $\beta_1, \ldots, \beta_k$ sont des entiers naturels tels que $0 \leqslant \beta_1 \leqslant \alpha_1, \ldots, 0 \leqslant \beta_k \leqslant \alpha_k$.

Réciproquement, un tel entier d est un diviseur de n car

$$n = \left(p_1^{\alpha_1 - \beta_1} \times \ldots \times p_k^{\alpha_k - \beta_k}\right) \times d.$$

Le résultat du 1) est démontré.

2) Puisque deux répartitions différentes des exposants $\beta_1, \ldots, \beta_k$ fournissent des diviseurs différents d'après le théorème fondamental de l'arithmétique, le nombre de diviseurs de n est aussi le nombre de répartitions d'exposants $\beta_1, \ldots, \beta_k$ où $0 \leqslant \beta_1 \leqslant \alpha_1, \ldots, 0 \leqslant \beta_k \leqslant \alpha_k$.

Pour chaque i tel que $1 \leqslant i \leqslant k$, il y a α_i entiers naturels compris au sens large entre 1 et α_i et donc il y a $\alpha_i + 1$ exposants β_i tels que $0 \leqslant \beta_i \leqslant \alpha_i$.
Il y a ensuite $(\alpha_1 + 1) \times \ldots \times (\alpha_k + 1)$ répartitions d'exposants $\beta_1, \ldots, \beta_k$ et finalement $(\alpha_1 + 1) \times \ldots \times (\alpha_k + 1)$ diviseurs de n.

Exemple. $72 = 2^3 \times 3^2$ admet $(3 + 1) \times (2 + 1) = 12$ diviseurs. Ce sont les nombres

$2^0 \times 3^0 = 1$	$2^1 \times 3^0 = 2$	$2^2 \times 3^0 = 4$	$2^3 \times 3^0 = 8$
$2^0 \times 3^1 = 3$	$2^1 \times 3^1 = 6$	$2^2 \times 3^1 = 12$	$2^3 \times 3^1 = 24$
$2^0 \times 3^2 = 9$	$2^1 \times 3^2 = 18$	$2^2 \times 3^2 = 36$	$2^3 \times 3^2 = 72$

La décomposition en facteur premier fournit aussi un procédé pour déterminer le PGCD de deux entiers.
On admettra le théorème suivant :

Théorème 32. Soient a et b deux entiers naturels supérieurs ou égaux à 2.
On pose $a = p_1^{\alpha_1} \times \ldots \times p_k^{\alpha_k}$ et $b = p_1^{\beta_1} \times \ldots \times p_k^{\beta_k}$ où $p_1, \ldots, p_k$ sont des nombres premiers deux à deux distincts et les exposants $\alpha_1, \ldots, \alpha_k, \beta_1, \ldots, \beta_k$ sont des entiers naturels éventuellement nuls.
Le PGCD de a et b est :

$$d = p_1^{\gamma_1} \times \ldots \times p_k^{\gamma_k},$$

où pour chaque i tel que $1 \leqslant i \leqslant k$, γ_i est le plus petit des deux entiers α_i et β_i.

Commentaire. Dans le théorème précédent, l'écriture $a = p_1^{\alpha_1} \times \ldots \times p_k^{\alpha_k}$ n'est pas nécessairement la décomposition primaire de n car certains exposants ont le droit d'être égaux à 0. Dit autrement, les nombres $p_1, \ldots, p_k$ ne sont peut-être pas tous des facteurs premiers de a.
Les nombres $p_1, \ldots, p_k$ sont les nombres premiers qui sont des facteurs premiers de a ou de b. ❑

Exemple. Soient $a = 4116$ et $b = 6300$. On a

$$a = 2^2 \times 3 \times 7^3 = 2^2 \times 3 \times 5^0 \times 7^3 \text{ et } b = 2^2 \times 3^2 \times 5^2 \times 7,$$

et donc

$$\text{PGCD}(a, b) = 2^2 \times 3 \times 5^0 \times 7 = 84.$$

VI. Congruences

1) Définition des congruences

Définition 7. Soit n un entier naturel. Soient a et b deux entiers relatifs.
On dit que a est congru à b modulo n et on écrit $a \equiv b\ (n)$ si et seulement si $b - a$ est un multiple de n.
Il revient au même de dire qu'il existe un entier relatif k tel que $b = a + kn$.

Remarque. Un cas particulier important de la définition 7 est

$$a \text{ est un multiple de } n \text{ si et seulement si } a \equiv 0\ (n).$$

Exemple. Puisque $17 - 1 = 16 = 4 \times 4$, $17 - 1$ est un multiple de 4 et donc

$$17 \equiv 1\ (4).$$

On peut aussi écrire : puisque $17 = 1 + 4 \times 4$, il existe un entier relatif k tel que $17 = 1 + 4k$ et donc $17 \equiv 1\ (4)$.

Théorème 33. Soit n un entier naturel non nul. Soient a et b deux entiers relatifs.
a et b sont congrus modulo n si et seulement si les restes des divisions euclidiennes de a et b par n sont les mêmes.

Démonstration. Soit n un entier naturel non nul. Soient a et b deux entiers relatifs.

La division euclidienne de a par n s'écrit $a = q_1 n + r_1$ avec q_1 et r_1 entiers relatifs tels que $0 \leqslant r_1 \leqslant n - 1$ et la division euclidienne de b par n s'écrit $b = q_2 n + r_2$ avec $0 \leqslant r_2 \leqslant n - 1$ avec q_2 et r_2 entiers relatifs tels que $0 \leqslant r_2 \leqslant n - 1$. En retranchant membre à membre, on obtient

$$b - a = (q_2 - q_1)n + (r_2 - r_1).$$

• Supposons que les restes r_1 et r_2 soient les mêmes. Alors, $r_2 - r_2 = 0$

$$b - a = (q_2 - q_1)n.$$

Puisque $q_2 - q_1$ est un entier relatif, $b - a$ est un multiple de n et donc $a \equiv b\ (n)$.

• Supposons que $a \equiv b\ (n)$. Il existe un entier relatif k tel que $b - a = kn$. L'égalité $b - a = (q_2 - q_1)n + (r_2 - r_1)$ s'écrit alors

$$kn = (q_2 - q_1)n + (r_2 - r_1),$$

puis

$$r_2 - r_1 = (q_1 - q_2 + k)n.$$

D'autre part, puisque $0 \leqslant r_1 < n$ et $0 \leqslant r_2 < n$, on a encore $-n < -r_1 \leqslant 0$ et $0 \leqslant r_2 < n$ puis en additionnant membre à membre, on obtient $-n < r_2 - r_1 < n$. Puisque $r_2 - r_1 = (q_1 - q_2 + k)n$, on a $-n < (q_1 - q_2 + k)n < n$ puis après simplification par l'entier strictement positif n, on obtient

$$-1 < q_1 - q_2 + k < 1.$$

Puisque $q_1 - q_2 + k$ est un entier relatif, ceci impose $q_1 - q_2 + k = 0$ ou encore $q_2 - q_1 = k$.
L'égalité $b - a = (q_2 - q_1)n + (r_2 - r_1)$ fournit alors $kn = kn + (r_2 - r_1)$ puis $r_2 - r_1 = 0$ et donc $r_1 = r_2$.

---

2) Propriétés des congruences

Théorème 34. Soit n un entier naturel.
1) Pour tout entier relatif a, $a \equiv a\ (n)$.
2) Pour tous entiers relatifs a et b, si $a \equiv b\ (n)$, alors $b \equiv a\ (n)$.
2) Pour tous entiers relatifs a, b et c, si $a \equiv b\ (n)$ et $b \equiv c\ (n)$, alors $a \equiv c\ (n)$.

Démonstration. Soit n un entier naturel.

1) Soit a un entier relatif. Alors, $a - a = 0 = 0 \times 0$ et donc il existe un entier relatif k tel que $a - a = 0 \times k$. On en déduit que $a \equiv a\ (n)$.

2) Soient a et b deux entiers relatifs. Supposons que $a \equiv b\ (n)$. Alors il existe un entier relatif k tel que $b - a = kn$. On en déduit que $a - b = (-k)n$ et donc que $a - b$ est un multiple de n puisque $-k$ est un entier relatif. Puisque $a - b$ est un multiple de n, on a donc $b \equiv a\ (n)$.

3) Soient a, b et c trois entiers relatifs. Supposons que $a \equiv b\ (n)$ et $b \equiv c\ (n)$. Il existe un entier relatif k tel que $b - a = kn$ et un entier relatif k' tel que $c - b = k'n$.
En additionnant membre à membre ces deux égalités, on obtient $c - a = (k + k')n$. Puisque $k + k'$ est un entier relatif, on a montré que $c - a$ est un multiple de n et donc que $a \equiv c\ (n)$.

Ainsi, les congruences se manipulent approximativement comme une égalité : une congruence se lit indifféremment de gauche à droite ou de droite à gauche, si a et congru à b et b est congru à c, alors a est congru à c ...

Le théorème suivant permet d'additionner un même nombre aux deux membres d'une congruence ou de multiplier ces deux membres par un même nombre.

Théorème 35. Soit n un entier naturel.
1) Pour tous entiers relatifs a, b et c, si $a \equiv b\ (n)$ alors $a + c \equiv b + c\ (n)$.
2) Pour tous entiers relatifs a, b et c, si $a \equiv b\ (n)$ alors $a \times c \equiv b \times c\ (n)$.

Démonstration. Soit n un entier naturel. Soient a, b et c trois entiers relatifs. Supposons que $a \equiv b\ (n)$. Alors il existe un entier relatif k tel que $b - a = kn$.

1) On a $(b + c) - (a + c) = b - a = kn$. Puisque $(b + c) - (a + c)$ est un multiple de n, on a donc $a + c \equiv b + c\ (n)$.

2) On a $(b \times c) - (a \times c) = c(b - a) = (ck)n$. Puisque ck est un entier relatif, on a montré que $(b \times c) - (a \times c)$ est un multiple de n et donc que $a \times c \equiv b \times c\ (n)$.

Une conséquence importante du théorème précédent est que l'on peut additionner membre ou multiplier membre à membre des congruences :

Théorème 36. Soit n un entier naturel.
1) Pour tous entiers relatifs a, b, c et d, si $a \equiv b\ (n)$ et $c \equiv d\ (n)$, alors $a + c \equiv b + d\ (n)$.
2) a) Pour tous entiers relatifs a, b, c et d, si $a \equiv b\ (n)$ et $c \equiv d\ (n)$, alors $a \times c \equiv b \times d\ (n)$.
b) Pour tous entiers relatifs a et b et tout entier naturel k, si $a \equiv b\ (n)$, alors $a^k \equiv b^k\ (n)$.

Démonstration. Soit n un entier naturel. Soient a, b, c et d quatre entiers relatifs. Supposons que $a \equiv b\ (n)$ et $c \equiv d\ (n)$.

1) On ajoute c aux deux membres de la première congruence et on ajoute b aux deux membres de la deuxième congruence. D'après le théorème précédent, on a $a + c \equiv b + c\ (n)$ et $b + c \equiv b + d\ (n)$. Le théorème 34 permet alors d'affirmer que $a + c \equiv b + d\ (n)$.

2) a) On multiplie par c les deux membres de la première congruence et on multiplie par b les deux membres de la deuxième congruence. D'après le théorème précédent, on a $a \times c \equiv b \times c\ (n)$ et $b \times c \equiv b \times d\ (n)$. Le théorème 34 permet alors d'affirmer que $a \times c \equiv b \times d\ (n)$. b) se démontre alors par récurrence grâce à a).

Exercice 7. Soit n un entier naturel non nul. On suppose que

$$n = c_p \times 10^p + c_{p-1}10^{p-1} + \ldots + c_1 \times 10 + c_0$$

où c_0, c_1, ..., c_p sont des entiers naturels compris au sens large entre 0 et 9 et $c_p \neq 0$ (c_0, c_1, ..., c_p sont les chiffres de l'écriture décimale de n).

Montrer que n est congru à la somme de ses chiffres modulo 9 et en déduire que n est divisible par 9 si et seulement si la somme des chiffres de n est divisible par 9.

Solution. $10 \equiv 1\ (9)$ et donc, pour tout entier naturel k, $10^k \equiv 1^k\ (n)$ ou encore $10^k \equiv 1\ (9)$.
Par suite, $c_p \times 10^p + c_{p-1}10^{p-1} + \ldots + c_1 \times 10 + c_0 \equiv c_p \times 1 + c_{p-1}10^{p-1} + \ldots + c_1 \times 1 + c_0\ (9)$ ou encore

$$n \equiv c_p + \ldots + c_1 + c_0\ (9).$$

En particulier,

$$n \text{ divisible par } 9 \Leftrightarrow n \equiv 0\ (9) \Leftrightarrow c_p + \ldots + c_1 + c_0 \equiv 0\ (9) \Leftrightarrow c_p + \ldots + c_1 + c_0 \text{ divisible par } 9$$

Par exemple, si $n = 64413$ alors la somme des chiffres de n est

$$6 + 4 + 4 + 1 + 3 = 18 = 2 \times 9.$$

La somme des chiffres de n est divisible par 9 et donc n est divisible par 9. On a effectivement $64413 = 7157 \times 9$.

3) Résolution de congruences

On se donne n un entier naturel et a, b et x trois entiers relatifs et on veut résoudre la congruence $ax + b \equiv 0\ (n)$ d'inconnue x. On va apprendre à « faire passer a et b de l'autre côté » quand cela est possible. On va voir que la multiplication est beaucoup plus délicate à gérer que l'addition.

• **Résolution de $x + a \equiv 0\ (n)$.** Soient n un entier relatif et a et x deux entiers relatifs.
Si $x + a \equiv 0\ (n)$, d'après le théorème 35, on a $x + a - a \equiv 0 - a\ (n)$ ou encore $x \equiv -a\ (n)$.
Si $x \equiv -a\ (n)$, alors $x + a \equiv a - a\ (n)$ et donc $x + a \equiv 0\ (n)$. En résumé,

$$x + a \equiv 0\ (n) \Leftrightarrow x \equiv -a\ (n).$$

• **Résolution de $ax \equiv b\ (n)$.** Soient n un entier relatif et a, b et x trois entiers relatifs.

Supposons il existe un entier relatif a' tel que $a \times a' \equiv 1\ (n)$ (on dit dans ce cas que a est inversible modulo n), alors on peut écrire :
si $ax \equiv b\ (n)$, d'après le théorème 35, on a $aa'x \equiv ba'\ (n)$ ou encore $1 \times x \equiv ba'\ (n)$ ou enfin $x \equiv ba'\ (n)$
et si $x \equiv ba'\ (n)$, alors $ax \equiv baa'\ (n)$ ou encore $ax \equiv b \times 1\ (n)$ et donc $ax \equiv b\ (n)$.

En résumé, s'il existe un entier relatif a' tel que $a \times a' \equiv 1\ (n)$, alors

$$ax \equiv b\ (n) \Leftrightarrow x \equiv ba'\ (n).$$

Exercice 8. 1) Résoudre dans $\mathbb{Z}$ la congruence $2x + 5 \equiv 0\ (7)$.
2) Montrer que la congruence $2x \equiv 1\ (6)$ n'a pas de solution dans $\mathbb{Z}$.

Solution. 1) Soit x un entier relatif. Si $2x + 5 \equiv 0\ (7)$, alors $2x + 5 - 5 \equiv 0 - 5\ (7)$ ou encore $2x \equiv -5\ (7)$ et si $2x \equiv -5\ (7)$, alors $2x + 5 \equiv -5 + 5\ (7)$ et donc $2x + 5 \equiv 0\ (7)$. En résumé,

$$2x + 5 \equiv 0\ (7) \Leftrightarrow 2x \equiv -5\ (7).$$

On note alors que $2 \times 4 = 8 = 1 + 7$ et donc que $2 \times 4 \equiv 1\ (7)$.
Si $2x \equiv -5\ (7)$, alors $4 \times 2x \equiv -5 \times 4\ (7)$ ou encore $x \equiv -20\ (7)$ et si $x \equiv -20\ (7)$, alors $2x \equiv -5 \times 4 \times 2\ (7)$ ou encore $2x \equiv -5\ (7)$. En résumé,

$$2x + 5 \equiv 0\ (7) \Leftrightarrow 2x \equiv -5\ (7) \Leftrightarrow x \equiv -20\ (7).$$

Enfin, comme $-20 \equiv 1\ (7)$ car $-20 - 1 = -21 = (-3) \times 7$,

$$2x + 5 \equiv 0\ (7) \Leftrightarrow x \equiv 1\ (7).$$

Les entiers relatifs x tels que $2x + 5 \equiv 0\ (7)$ sont les entiers relatifs de la forme $1 + 7k$ où k est un entier relatif.

2) Supposons qu'il existe un entier relatif x tel que $2x \equiv 1\ (6)$.
Alors, il existe un entier relatif k tel que $2x = 1 + 6k = 1 + 2 \times (3k)$. Le membre de gauche de cette égalité est un entier pair et le membre de droite est un entier impair. Ceci est impossible et donc la congruence $2x \equiv 1\ (6)$ n'a pas de solution dans $\mathbb{Z}$.